Wajah Hukum

Vol 9, No 2 (2025): Oktober, 880-888
Fakultas Hukum Universitas Batanghari Jambi
ISSN 2598-604X (Online) | DOI 10.33087/wjh.v9i2.1949

Aspek Hukum Peran TNI Mengatasi Serangan Siber dalam Rangka Pertahanan Keamanan Nasional

Fauziah Nauri Qisty, Bayu Setiawan, Anang Puji Utama
Fakultas Keamanan Nasional, Universitas Pertahanan Republik Indonesia
Correspondence: fauziah.qisty@kn.idu.ac.id, bayu.setiawan1961@gmail.com, anang.utama@idu.ac.id.

Article Info
Submitted: *30-07-2025*
Revised: *31-07-2025*
Accepted: *27-10-2025*
Published: *27-10-2025*

Keywords:
Legal Aspects; Indonesian National Army; Threat; Attack; Cyber.

Abstract
Cyberattacks are a growing and increasingly threatening form of non-traditional threat that endangers national security stability in the digital age. In this context, cybersecurity has become an integral part of the nation's defense system, making the role of the Indonesian National Army (TNI) in facing cyberattacks increasingly relevant and urgent. However, the legal aspects governing the authority of the Indonesian National Armed Forces (TNI) in the cyber domain still raise debate, particularly due to the lack of comprehensive and specific regulations. This research aims to examine and understand the legal basis governing the role of the Indonesian National Armed Forces (TNI) in addressing cyber threats, analyze the limits of its legal authority within the context of national cyber defense, and evaluate the implementation of existing policies. This research uses a normative juridical method, as well as relevant legislation (statute approach) and conceptual (conceptual approach) approaches. The research results indicate that although the role of the Indonesian National Armed Forces (TNI) is highly strategic in facing covert and high-risk cyber threats to national sovereignty, the involvement of the TNI must be based on a clear and firm legal framework, carried out through effective coordination with relevant institutions, and always uphold applicable legal principles.

Kata Kunci:
Aspek Hukum; TNI; Ancaman; Serangan; Siber.

Abstrak
Serangan siber merupakan bentuk ancaman nontradisional yang kian berkembang dan mengancam stabilitas keamanan nasional di era digital. Dalam konteks ini, keamanan siber menjadi bagian integral dari sistem pertahanan negara, sehingga peran Tentara Nasional Indonesia (TNI) dalam menghadapi serangan siber semakin relevan dan mendesak. Namun demikian, aspek hukum yang mengatur kewenangan TNI dalam domain siber masih menimbulkan perdebatan, terutama akibat belum tersusunnya regulasi yang komprehensif dan spesifik. Penelitian ini bertujuan untuk mengkaji dan memahami landasan hukum yang mengatur peran TNI dalam menangani ancaman siber, menganalisis batas-batas kewenangan hukumnya dalam konteks pertahanan siber nasional, serta mengevaluasi implementasi kebijakan yang telah berlaku. Penelitian ini menggunakan metode yuridis normatif, dan pendekatan perundang-undangan (*statute approach*) juga pendekatan konseptual (*conceptual approach*) yang relevan. Hasil penelitian menunjukkan bahwa meskipun peran TNI sangat strategis dalam menghadapi ancaman siber yang bersifat terselubung dan berisiko tinggi terhadap kedaulatan negara, pelibatan TNI harus didasarkan pada kerangka hukum yang jelas dan tegas, serta dilakukan melalui koordinasi yang efektif dengan institusi terkait dan tetap menjunjung tinggi prinsip-prinsip hukum yang berlaku.

PENDAHULUAN

Keamanan nasional tidak lagi hanya dihadapkan pada ancaman militer konvensional yang bersifat terbuka dan teridentifikasi secara jelas. Dalam perkembangannya, Indonesia menghadapi berbagai bentuk ancaman terselubung yang sifatnya kompleks, tidak kasat mata, dan sering kali melibatkan aktor non-negara maupun infiltrasi kekuatan asing. Ancaman semacam ini dapat muncul melalui jalur ideologi, ekonomi, siber, informasi, dan bahkan budaya. Dalam konteks tersebut, stabilitas nasional dapat terganggu tanpa adanya aksi militer secara langsung, tetapi melalui pengaruh yang melemahkan kedaulatan negara dari dalam secara perlahan.

Salah satu bentuk ancaman terselubung yang semakin mengemuka di Indonesia adalah serangan siber (*cyber attack*). Serangan ini umumnya menyasar infrastruktur digital negara, seperti sistem data kependudukan, layanan publik, pertahanan, hingga keuangan. Serangan siber bersifat lintas batas, sulit dilacak, dan sering kali dilakukan secara sistematis dengan tujuan mengganggu kestabilan nasional, mencuri data sensitif, atau bahkan mengendalikan opini publik melalui manipulasi informasi.[1] Beberapa insiden besar dalam beberapa tahun terakhir menunjukkan bahwa Indonesia masih sangat rentan terhadap ancaman ini, termasuk serangan terhadap data instansi pemerintah dan kebocoran data digital berskala besar.

Ancaman siber kini memainkan peran strategis dalam dinamika geopolitik, khususnya di kawasan Asia Tenggara, di mana negara-negara besar seperti Amerika Serikat, Tiongkok, dan Rusia memanfaatkan kemampuan siber demi melindungi kepentingan politik dan ekonominya. Indonesia, yang memiliki posisi geografis penting di kawasan Samudra Hindia dan Pasifik, menjadi rentan terhadap dinamika ini, sehingga aktif berpartisipasi dalam berbagai forum internasional seperti PBB, ASEAN, dan APEC-TEL untuk menyeimbangkan dominasi kekuatan siber global. Serangan siber telah menjadi bagian nyata dari peperangan modern, seperti yang terlihat dari insiden besar yang melibatkan Rusia di Estonia dan Georgia, Korea Utara terhadap Korea Selatan, serta serangan siber yang mengiringi invasi Rusia ke Ukraina pada tahun 2022. Serangan terhadap Israel pada tahun 2023 juga memperkuat posisi ruang siber sebagai arena penting dalam konflik global dan menjadikannya komponen integral dalam strategi militer masa kini.[2]

Di Indonesia, eskalasi serangan siber meningkat sejak pandemi Covid-19, yang mempercepat adopsi teknologi digital dan memunculkan ancaman siber sebagai tantangan aktual dalam situasi global. Dalam periode 2020-2024, Indonesia menghadapi insiden besar, termasuk dugaan sabotase terhadap PLN pada tahun 2019 dengan kerugian Rp90 miliar, serangan ransomware Lockbit 3.0 terhadap BSI pada tahun 2023 serta rentetan aksi peretasan oleh "Bjorka" pada tahun 2022 sampai dengan 2024 terhadap Tokopedia, KPU, dan data registrasi SIM Card Kemenkominfo. Kemudian yang tidak kalah merugikan negara dan masyarakat yaitu insiden pada September 2024 yang mencakup bocornya 6 juta data NPWP DJP Kemenkeu dan serangan ransomware Lockbit 3.0 terhadap PDNS 2 SPBE yang menggemparkan nasional dan internasional.[3]

Berdasarkan Perpres 82 Tahun 2022, sektor Pertahanan Indonesia sebagai Infrastruktur Informasi Vital harus dilindungi dari ancaman siber besar yang dapat merusak kepentingan publik, keamanan, dan perekonomian nasional. Krisis siber, yang dapat menyebabkan kelumpuhan operasional negara, seperti pencurian data massal dan disrupsi ekonomi, memerlukan upaya pertahanan siber yang lebih kuat, termasuk penguatan kemitraan internasional. Pemerintah telah mengambil langkah strategis melalui pembentukan Badan Siber dan Sandi Negara, penguatan NSOC, serta pembentukan 121 CSIRT, namun implementasi masih menghadapi tantangan, seperti kurangnya koordinasi dalam merespons insiden besar seperti serangan Bjorka dan PDNS 2.[4] Meskipun telah ada Undang-Undang Perlindungan Data Pribadi dan Peraturan Manajemen Krisis Siber, kebijakan ini belum berjalan maksimal karena belum ada deklarasi status krisis oleh pemerintah.

Dalam menyikapi ancaman terselubung krisis serangan siber ini dirasa perlu melibatkan TNI. Sebagai komponen utama dalam sistem pertahanan negara, TNI memiliki peran strategis dalam menjaga kedaulatan dan integritas nasional melalui pertahanan siber. Dalam konteks ini, TNI tidak hanya berperan sebagai pelaksana teknis, tetapi juga sebagai aktor yang harus beroperasi dalam koridor hukum yang jelas. Peraturan perundang-undangan seperti Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia dan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan

[1] Destya Fitri, dkk, "Peranan Manajemen Sekuriti Terhadap Keamanan Cyber Bersumber Nilai-Nilai Kebangsaan UUD 1945 Dalam Meningkatkan Efektivitas di Era Digitalisasi untuk Keamanan Nasional", *Menawan: Jurnal Riset dan Publikasi Ilmu Ekonomi, Vol. 3, No. 2,* (2024) : 273-283.

[2] Prabaswari, "Pengembangan Model Kapabilitas Tanggap Insiden Siber Sektor Pertahanan dalam Mengantisipasi Krisis Siber Nasional", *Disertasi, Program Studi Ilmu Pertahanan*, (Bogor : Unhan RI, 2025), dipublikasikan.

[3] *Ibid.*

[4] *Ibid.*

Transaksi Elektronik menjadi dasar bagi TNI dalam menjalankan tugasnya di ranah siber.[5] Selain itu, Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga memberikan landasan bagi pengelolaan dan pengamanan sistem elektronik yang vital bagi negara.[6]

Pentingnya peran TNI dalam pertahanan siber juga ditegaskan oleh Panglima TNI, yang menyatakan bahwa TNI memberdayakan semua potensi Sumber Daya Siber Nasional dalam melaksanakan fungsi pengawasan dan pengendalian sistem keamanan terpadu yang terintegrasi dengan seluruh komponen bangsa. Namun, tantangan yang dihadapi tidak hanya bersifat teknis, tetapi juga berkaitan dengan aspek hukum, etika, dan koordinasi antar lembaga.

Penelitian ini bertujuan untuk menganalisis bagaimana peran TNI dalam mengatasi ancaman terselubung serangan siber dalam pertahanan keamanan negara dan bagaimana Aspek Hukum peran TNI dalam mengatasi ancaman terselubung serangan siber dan apa saja kendala hukum dalam mengimplementasikannya di dalam kehidupan bermasyarakat.

METODE

1. Pendekatan

   Penelitian ini juga menggunakan metode pendekatan yuridis normatif yaitu penelitian hukum yang dilakukan dengan cara menelaah bahan-bahan hukum primer dan sekunder yang lebih memfokuskan pada analisis norma-norma hukum yang berlaku. Pendekatan yang digunakan dalam penelitian ini adalah pendekatan perundang-undangan (*statute approach*) dan pendekatan konseptual (*conceptual approach*), dengan mengkaji peraturan perundang-undangan yang relevan seperti Undang-Undang TNI, Undang-Undang Pertahanan Negara, dan regulasi terkait keamanan siber di Indonesia.
2. Rencana Kegiatan

   Rencana kegiatan dalam suatu penelitian yaitu guna mempersiapkan penelitian yang akan diteliti oleh penulis. Adapun rencana kegiatan yang akan dilakukan oleh penulis adalah menganalisis aspek hukum peran TNI dalam penanganan kasus serangan siber.
3. Ruang lingkup atau Objek

   Penelitian ini secara khusus mengkaji peran Tentara Nasional Indonesia (TNI) dalam menghadapi ancaman siber yang bersifat terselubung sebagai bagian dari upaya pertahanan negara. Objek utama yang diteliti adalah aspek hukum yang mengatur kewenangan TNI dalam domain pertahanan siber, termasuk bagaimana batas-batas legalitas tindakan TNI diatur dalam peraturan perundang-undangan nasional. Ruang lingkup penelitian meliputi analisis terhadap regulasi yang telah berlaku, implementasi kebijakan pertahanan siber, serta relevansi pelibatan TNI dalam konteks keamanan nasional yang semakin terancam oleh serangan digital. Dengan demikian, fokus penelitian ini mencakup keterkaitan antara dinamika ancaman siber, regulasi hukum nasional, dan posisi strategis TNI dalam sistem keamanan negara.
4. Bahan dan Alat Utama

   Bahan utama yang digunakan mencakup bahan hukum primer, seperti Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain itu, digunakan juga bahan hukum sekunder berupa literatur ilmiah, artikel jurnal, serta laporan institusi pemerintah dan organisasi internasional yang relevan. Alat analisis utama dalam penelitian ini adalah analisis isi (*content analysis*), yang digunakan untuk menelaah substansi norma hukum serta keterkaitannya dengan praktik pertahanan siber oleh TNI, dengan pendekatan deskriptif-analitis untuk menjelaskan dan mengevaluasi regulasi yang ada.
5. Tempat

   Karena penelitian ini bersifat normatif dan berbasis studi kepustakaan, maka pelaksanaannya tidak memerlukan observasi langsung di lapangan atau laboratorium. Tempat penelitian bersifat non-

[5] https://theconversation.com/pertahanan-siber-indonesia-jadi-tugas-penting-panglima-tni-yang-baru-171599, diakses tanggal 20 Juli 2025.

[6] https://news.republika.co.id/berita/qtre0w396/panglima-tni-berdayakan-semua-potensi-daya-siber-nasional, diakses tanggal 20 Juli 2025.

fisik dan dilakukan melalui pengumpulan data dari berbagai sumber dokumen hukum dan ilmiah. Lokasi penelitian mencakup perpustakaan hukum, situs resmi pemerintah dan portal akademik.

6. Teknik Pengumpulan Data

   Penelitian ini menerapkan teknik pengumpulan data dengan studi kepustakaan yang meliputi peraturan perundang-undangan dan buku-buku literatur pendukung dengan mencari dan mempelajari data, dokumen atau bahan pustaka lainnya yang berkaitan dengan serangan siber dan pertahanan negara.

7. Definisi Operasional Variabel Penelitian

   Dalam penelitian ini definisi operasional variabel adalah suatu penjelasan yang berkaitan dengan istilah yang digunakan dalam judul penelitian supaya penulis dapat memberikan pemahaman dalam penelitian ini. Adapun variabel pertama dalam penelitian ini adalah Peran TNI dalam Pertahanan Siber, yang didefinisikan sebagai bentuk keterlibatan institusional TNI dalam mencegah, menanggulangi, dan merespons serangan siber terhadap kepentingan strategis nasional, termasuk perlindungan terhadap infrastruktur digital negara. Variabel kedua adalah Aspek Hukum, yang merujuk pada keseluruhan kerangka peraturan perundang-undangan yang mengatur batas kewenangan, prosedur pelibatan, serta prinsip-prinsip hukum yang harus ditaati TNI dalam menjalankan tugasnya di ranah siber. Adapun variabel ketiga adalah Ancaman Siber, yang dioperasionalkan sebagai segala bentuk upaya yang dilakukan melalui media digital dan teknologi informasi untuk merusak, mencuri, atau mengganggu sistem dan data milik negara, baik dilakukan oleh aktor negara maupun non-negara, serta memiliki potensi mengganggu stabilitas dan kedaulatan nasional.

8. Teknik Analisis

   Penelitian ini menerapkan metode kualitatif dengan fokus pada kajian literatur hukum studi Pustaka. Sumber data yang digunakan mencakup jurnal ilmiah, portal berita, dokumen resmi pemerintah, serta sumber-sumber terpercaya lainnya yang berkaitan dengan isu serangan siber dan pertahanan negara. Kemudian penelitian ini menggunakan teknik analisis isi dan analisis deskriptif normatif. Analisis isi digunakan untuk menelaah dokumen hukum, kebijakan, dan literatur ilmiah yang berkaitan dengan kewenangan TNI dalam menghadapi ancaman siber. Teknik ini dilakukan dengan menggambarkan dan menjelaskan norma-norma hukum yang mengatur peran TNI dalam pertahanan siber berdasarkan teori hukum dan prinsip-prinsip konstitusional. Teknik ini juga digunakan untuk mengevaluasi sejauh mana regulasi yang ada memberikan dasar hukum yang jelas dan efektif bagi pelibatan TNI dalam merespons serangan siber, serta menilai kesesuaiannya dengan sistem hukum nasional dan standar internasional. Diharapkan, hasil dari penelitian ini dapat memberikan rekomendasi untuk penguatan regulasi dan strategi pertahanan siber nasional yang lebih efektif dan sesuai dengan prinsip-prinsip hukum yang berlaku.[7]

HASIL

Serangan Siber Dan Ancaman Terhadap Keamanan Nasional

Keamanan nasional dapat sangat bermanfaat jika didefinisikan sebagai kemampuan dari suatu bangsa untuk melindungi nilai-nilai internalnya dari ancaman pihak luar. Keamanan nasional bisa menjadi sebuah konsep yang digunakan untuk pemerintahan yang berkuasa dalam rangka mengamankan posisi atau status *quonya*. Keamanan nasional dapat didefinisikan sebagai suatu kondisi protektif yang para negarawan berusaha capai, atau jaga, dalam rangka mengamankan berbagai macam komponen politik dari ancaman dalam dan luar. Keamanan disini berarti usaha untuk mengurangi dampak dari ancaman atau bahaya, ancaman sendiri adalah sesuatu yang berpotensi mengganggu, menghalangi atau merusak nilai-nilai yang dianut atau dipercaya.[8] Upaya keamanan biasanya dilakukan dengan perlindungan dimana ini berarti kita terlepas dari penghalang, terbebas untuk dapat melakukan sesuatu yang bernilai bagi kita. Hal ini menjadikan Kepentingan nasional menjadi keamanan dengan mengacu pada hasil bernilai yang diinginkan oleh mereka yang berada dalam basis efektif politik dalam suatu bangsa, nilai seperti itu biasanya diasosiasikan dengan konsep kepentingan nasional.

[7] https://www.tni-au.mil.id/berita/detail/menjawab-tantangan-era-digital-tni-au-gelar-sosialisasi-aspek-hukum-penggunaan-siber-dalam-operasi-militer, diakses tanggal 20 Juli 2025.

[8] Tamarell Vimy, dkk, Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan, Vol. 6, No. 1*, (2022) : 2319-2327.

Indonesia memiliki kepentingan nasional yang menjadi landasan terbentuknya kebijakan dan strategi. Dengan itu, Indonesia menjadikan Pembukaan Undang-Undang Dasar 1945 alinea IV yang didalamnya terkandung kepentingan nasional Indonesia, yang pertama meliputi "Melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia", kedua "Memajukan kesejahteraan umum". Ketiga "Mencerdaskan kehidupan bangsa". Dan keempat ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial Keempat butir ini mampu dijadikan landasan setiap kebijakan serta strategi yang dibentuk oleh pemerintah. Perlindungan atas segenap bangsa menjadi kepentingan nasional yang sangat penting. Menurut Morgenthau, setiap negara harus melindungi teritorial bersamaan dengan politik untuk berhadapan dengan negara lain.

Di dunia yang terdiri dari banyak negara yang bersaing dan menentang untuk mendapatkan kekuasaan, kelangsungan hidup mereka adalah syarat mutlak dan minimum mereka. Kepentingan nasional dasar dapat digambarkan sebagai berikut:

- Kepentingan pertahanan: perlindungan negara-bangsa dan warganya terhadap ancaman kekerasan fisik yang diarahkan dari negara lain, dan / atau ancaman yang diilhami secara eksternal terhadap sistem pemerintahannya.
- Kepentingan ekonomi: peningkatan kesejahteraan ekonomi negara-bangsa dalam hubungannya dengan negara-negara lain.
- Kepentingan Tatanan Dunia: pemeliharaan sistem politik dan ekonomi internasional di mana negara-bangsa dapat merasa aman, dan di mana warga dan perdagangannya dapat beroperasi secara damai di luar perbatasannya.
- Kepentingan ideologis: perlindungan dan kelanjutan dari seperangkat nilai yang dimiliki dan dipercayai oleh orang-orang dari negara-bangsa secara universal.

Pola untuk menguasai suatu negara tidak lagi dilakukan secara frontal atau melalui perang konvensional militer dengan senjata, karena adanya hukum-hukum dan organisasi dunia, sehingga dilakukan dengan cara-cara *nonlinier*, tidak langsung, dan bersifat *proxy war*. Ancaman pertahanan dan keamanan negara saat ini cenderung mengarah pada sifat-sifat perang tanpa menggunakan senjata atau non-militer. Jika kita melihat berdasarkan fenomena yang ada saat ini pada beberapa negara salah satunya Indonesia banyak sekali serangan non-militer tetapi mengancam keamanan negara salah satunya yaitu serangan siber (*syber war*). Adapun serangan siber mencakup berbagai bentuk ancaman terhadap sistem komputer dan jaringan yang dapat merusak infrastruktur kritis negara. Menurut Fidler, serangan siber bisa memengaruhi sektor vital seperti energi, transportasi, dan layanan publik lainnya yang berhubungan langsung dengan kehidupan masyarakat. Dalam konteks Indonesia, serangan siber memiliki potensi besar untuk mengganggu kestabilan negara dan perekonomian. Oleh karena itu, penanganan ancaman ini memerlukan sinergi antara berbagai lembaga negara.[9]

Cyber crime dan *Cyber War* tidak hanya menjadi ancaman yang menyerang individu saja melainkan juga ancaman terhadap bidang bisnis dan industri serta objek vital pemerintahan. Pembuatan opini publik dan dunia internasional terhadap suatu maksud seperti untuk kampanye hingga propaganda. Dengan adanya teknologi informasi dan internet para pelaku ini dapat melakukannya dengan cara mudah, menggunakan biaya dan sumber daya yang lebih efisien. Kejadian terkait serangan siber adalah upaya spionase pada bidang industri dan objek vital pemerintah seperti penyanderaan dan perusakan informasi rahasia yang penting dapat menimbulkan rasa khawatir dan tidak aman karena kehilangan batas-batas pribadi dan ancaman kehilangan aset serta kekayaan. Tidak hanya itu jika upaya serangan siber ini terjadi maka dapat dimanfaatkan untuk kepentingan politik dunia siber juga dapat digunakan sebagai alat politik seperti penyebaran berita hoax dengan tujuan provokasi politis hingga rekayasa pada sektor perekonomian. Interkoneksi internet juga memungkinkan terjadinya serangan yang bertujuan melumpuhkan dan menghancurkan sumber daya negara lawan tanpa perlu mendekati objek tersebut.

Peran TNI dalam Pertahanan Siber

Penerapan pertahanan siber menjadi keniscayaan dan merupakan suatu prioritas kewajiban bagi negara dan semua instansi di dalamnya dimana tingkat pentingnya berbanding lurus dengan tingkat ketergantungan pada pemanfaatan di ruang siber tersebut. Hal ini menyebabkan Kemhan/TNI

[9] D. P. Fidler, "Cybersecurity and International Law: An Evolving Framework", *Journal of International Affairs, Vol. 72, No.1* (2018) : 475-493.

berkewajiban untuk mengambil langkah-langkah penting terkait dengan pertahanan siber, baik di dalam lingkungannya sendiri maupun dalam rangka mendukung pertahanan siber lintas sektoral. Pertahanan siber perlu dilaksanakan secara terencana dan terpadu agar penerapannya dapat berjalan secara tepat dan optimal berdasarkan Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.

Kementerian Pertahanan dan Tentara Nasional Indonesia memiliki dua kepentingan dalam pertahanan siber. Pertama, untuk mengamankan semua sistem elektronik dan jaringan informasi di lingkungannya. Kedua, mendukung koordinasi pengamanan siber di sektor-sektor lainnya sesuai kebutuhan. Memperhatikan dua kepentingan tersebut maka diperlukan antisipasi bagi kebutuhan pertahanan siber yang meliputi aspek-aspek yaitu sebagai berikut:

- Kebijakan
  Kebijakan-kebijakan yang menjadi acuan bagi seluruh kegiatan pertahanan siber termasuk pengembangan, pengoperasian dan koordinasi sangat penting untuk dirumuskan dan ditetapkan. Kebijakan-kebijakan ini meliputi aspek pengembangan kelembagaan, persiapan infrastruktur dan teknologi, persiapan Sumber Daya Manusia dan penetapan peran, fungsi dan wewenang dalam pertahanan siber di lingkungan Kemhan/TNI.
- Kelembagaan
  Kelembagaan yang kuat dan efektif sangat diperlukan dalam menjalankan tugas-tugas dan kegiatan pertahanan siber, dengan mengacu kepada kebijakan yang ditetapkan.
- Teknologi dan Infrastruktur pendukung
  Teknologi dan infrastruktur pendukung yang lengkap, diperlukan sebagai sarana dan kelengkapan bagi kegiatan pertahanan siber yang diselenggarakan, agar pertahanan siber dapat terlaksana dengan efektif dan efisien.
- Sumber Daya Manusia
  Sumber Daya Manusia merupakan satu unsur yang terpenting dalam memastikan terlaksananya pertahanan siber sesuai dengan kebijakan-kebijakan yang ditetapkan. Pengetahuan dan ketrampilan khusus pertahanan siber harus dimiliki dan dipelihara sesuai dengan perkembangan kondisi kebutuhan pertahanan siber. Sumber Daya Manusia diwujudkan dalam bentuk program rekruitmen, pembinaan serta pemisahan yang mengacu pada ketentuan yang berlaku.[10]

Berbicara tentang peran TNI, TNI memiliki peran yang cukup strategis dalam menjaga kedaulatan dan integritas negara, yang juga mencakup ancaman dari dunia maya. Sebagai bagian dari upaya untuk menjaga pertahanan negara, TNI telah mengembangkan doktrin pertahanan siber yang mencakup beberapa aspek hukum. Berdasarkan Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, TNI diberikan mandat untuk melaksanakan tugas-tugas pertahanan negara, termasuk menghadapi ancaman non-konvensional seperti serangan siber.[11] Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga memberikan landasan hukum untuk menangani serangan siber di Indonesia, dengan peran BSSN sebagai koordinator dalam upaya pertahanan dunia maya.

TNI dalam menghadapi serangan siber tidak bertindak sendiri, melainkan berkoordinasi dengan lembaga lain seperti Badan Siber dan Sandi Negara (BSSN) dan Kepolisian Negara Republik Indonesia (Polri). Hal ini penting untuk memastikan bahwa respons terhadap serangan siber dilakukan secara terintegrasi dan sesuai dengan hukum yang berlaku. Kemudian TNI juga mengembangkan doktrin pertahanan siber sebagai bagian dari strategi untuk melindungi negara dari ancaman dunia maya. Doktrin ini mencakup kebijakan mengenai deteksi, mitigasi, dan respons terhadap serangan siber yang dapat merusak sistem pemerintahan atau infrastruktur kritikal negara.[12]

Aspek Hukum Dalam Peran TNI Mengatasi Serangan Siber

Peran Tentara Nasional Indonesia (TNI) dalam mengatasi serangan siber memiliki dasar hukum yang kuat baik secara nasional maupun internasional. Di tingkat nasional, TNI berlandaskan Undang-

[10] *Ibid.*

[11] A. Suyanto, "Peran TNI dalam Penanggulangan Serangan Siber: Perspektif Hukum dan Keamanan Nasional", *Jurnal Hukum & Keamanan, Vol. 15, No. 2*, (2020).

[12] I. Setiawan, "Doktrin Pertahanan Siber TNI dalam Menghadapi Ancaman Non-Konvensional", *Jurnal Pertahanan dan Keamanan, Vol. 24, No.3*, (2019).

Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia yang menetapkan TNI sebagai alat negara di bidang pertahanan, termasuk dalam ruang siber. Peran ini semakin diperkuat dengan Peraturan Presiden Nomor 66 Tahun 2019 tentang Struktur Organisasi TNI yang menetapkan pembentukan Satuan Siber TNI (Satsiber TNI) guna melaksanakan operasi siber dalam mendukung tugas pokok pertahanan negara.[13]

Di ranah internasional, TNI juga berupaya menyesuaikan diri dengan prinsip hukum humaniter internasional (*International Humanitarian Law*) dan hukum hak asasi manusia internasional (*International Human Rights Law*) dalam setiap operasi siber. Upaya ini ditunjukkan dengan keterlibatan personel hukum TNI dalam kursus hukum siber internasional yang diselenggarakan oleh *Defense Institute of International Legal Studies* (DILS) Amerika Serikat.[14] Penegakan hukum terhadap pelaku serangan siber, terutama yang melibatkan aktor internasional, membutuhkan kerja sama antar negara. Dalam hal ini, Indonesia perlu memastikan bahwa langkah yang diambil TNI tidak hanya efektif dalam mengatasi ancaman, tetapi juga sesuai dengan hukum internasional yang mengatur penggunaan teknologi dalam konflik.[15]

Kemudian hubungan antar kelembagaan juga menjadi aspek penting dalam menghadapi serangan siber. TNI bekerja sama dengan Badan Siber dan Sandi Negara (BSSN), Kominfo, dan BIN, termasuk melalui pembentukan tim tanggap insiden siber (CSIRT) di berbagai lingkungan kementerian dan lembaga, termasuk TNI. Selain itu, aspek pendidikan dan pelatihan hukum siber bagi personel TNI juga menjadi fokus penting untuk meningkatkan pemahaman tentang tata kelola operasi siber sesuai ketentuan hukum nasional dan internasional. TNI AU, misalnya, secara aktif menyelenggarakan sosialisasi mengenai aspek hukum penggunaan siber dalam operasi militer, yang bertujuan meningkatkan kesadaran hukum di kalangan prajurit.

Seiring kompleksitas ancaman siber yang semakin berkembang, muncul juga gagasan untuk melakukan amandemen terhadap Undang-Undang Dasar 1945 guna mengakomodasi pembentukan angkatan siber sebagai senjata baru dalam struktur TNI. Langkah ini dinilai penting untuk memperkuat legitimasi dan struktur hukum dalam pelaksanaan peran pertahanan siber yang dijalankan oleh TNI secara komprehensif dan profesional. Dengan dasar hukum yang jelas serta koordinasi antar sektor yang kuat, TNI diharapkan mampu menjalankan tugasnya dalam menjaga kedaulatan dan keamanan nasional di ruang siber secara efektif dan sesuai hukum.

Kendala Hukum Dalam Implementasi Peran TNI Dalam Pertahanan Siber

Implementasi peran Tentara Nasional Indonesia (TNI) dalam pertahanan siber menghadapi sejumlah kendala hukum. Salah satu isu utama adalah kurang memadainya dasar hukum yang mengatur peran TNI di ruang siber. Meskipun ada sejumlah peraturan yang mengatur peran TNI dalam pertahanan siber, namun regulasi yang ada masih belum cukup mengakomodasi kompleksitas ancaman siber yang terus berkembang. Hal ini membutuhkan pembaruan dan penguatan regulasi agar lebih efektif dalam menghadapi ancaman. Seperti Undang-Undang Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia tidak secara tegas mencakup peran TNI dalam siber, yang menyebabkan tumpang tindih kewenangan dengan lembaga lain seperti Badan Siber dan Sandi Negara (BSSN).[16]

Selain itu terdapat beberapa kendala lagi terkait pembentukan regulasi yang terbaru yaitu terkait dengan wacana revisi Undang-Undang Nomor 34 Tahun 2004 tentang TNI (UU TNI). Koalisi Masyarakat Sipil menilai bahwa revisi tersebut berpotensi mengembalikan praktik dwifungsi ABRI, di mana militer aktif dapat menduduki jabatan sipil di luar fungsi pertahanan negara. Salah satu poin kontroversial dalam draf revisi adalah perluasan jabatan sipil yang dapat diduduki oleh prajurit TNI aktif. Pada Pasal 47 Ayat (2) dalam draf tersebut mengusulkan penambahan frasa "serta kementerian/lembaga lain yang membutuhkan tenaga dan keahlian prajurit aktif sesuai dengan

[13] https://www.antaranews.com/berita/2538541/profesionalisme-tni-pada-era-pertahanan-siber, diakses tanggal 20 Juli 2025.

[14] https://tniad.mil.id/dua-perwira-hukum-tni-ad-mengikuti-cyber-law-course-kerja-sama-ri-as/, diakses tanggal 20 Juli 2025.

[15] M. Murphy, "Cyber Warfare and International Law: The Rules of Engagement". *International Law Review. Vol. 21, No. 4*, (2020).

[16] https://nasional.kompas.com/read/2024/09/26/05150011/wacana-angkatan-siber-sejauh-mana-uu-pertahanan-dan-tni-direvisi-, diakses tanggal 20 Juli 2025.

kebijakan Presiden". Koalisi Masyarakat Sipil menilai bahwa perubahan ini membuka peluang bagi prajurit TNI aktif untuk ditempatkan di kementerian dan lembaga di luar 10 yang telah ditetapkan dalam UU TNI, sehingga mengaburkan batas antara ranah militer dan sipil.[17]

Dalam konteks pertahanan siber, penempatan prajurit TNI aktif di lembaga sipil yang tidak memiliki kaitan langsung dengan pertahanan negara dapat menimbulkan konflik kepentingan dan mengurangi profesionalisme TNI. Hal ini juga berisiko mengurangi kesempatan bagi Aparatur Sipil Negara (ASN) dan perempuan dalam mengakses jabatan strategis, serta memperkuat dominasi militer dalam pemerintahan. Tetapi dibalik isu ini, RUU TNI ini memiliki relevansi yang cukup erat dalam mengahadapi ancaman siber nasional. Berikut adalah beberapa relevansinya:

- Penegasan Siber sebagai Domain Strategis Pertahanan: Secara eksplisit mengakui ruang siber sebagai domain operasi keempat, legitimasi keterlibatan TNI menangani serangan, melindungi infrastruktur digital, hingga melakukan kontra-serangan.
- Pengembangan SDM TNI yang Adaptif dan Strategis: RUU mendorong SDM siber TNI yang handal, siap di sistem komando krisis, dan adaptif terhadap ancaman digital kompleks.
- Dorongan Kemandirian Teknologi Keamanan Siber: Memperkuat urgensi teknologi keamanan asing dan menjaga kedaulatan digital.
- Penguatan Struktur dan Kapasitas Siber TNI: Membuka ruang penguatan satuan siber TNI dari fungsi administratif menjadi kekuatan strategis.[18]

Kemudian selain kendala hukum terhadap krisis siber tingkat nasional, terdapat kendala terhadap penanganan serangan siber yang melibatkan aktor internasional yaitu memerlukan kerja sama yang lebih erat dengan negara-negara lain. Namun, hal ini terkendala oleh perbedaan pandangan dan regulasi yang ada di masing-masing negara. Untuk mengatasi kendala-kendala tersebut, diperlukan revisi regulasi yang melibatkan berbagai pihak, termasuk masyarakat dan ahli, guna memastikan bahwa peran TNI dalam pertahanan siber tidak hanya efektif tetapi juga sah secara hukum dan tidak mengancam kebebasan digital masyarakat.

SIMPULAN

Berdasarkan hasil penelitian, dapat disimpulkan bahwa serangan siber merupakan bentuk ancaman nontradisional yang semakin berkembang dan membahayakan stabilitas keamanan nasional. Dalam menghadapi ancaman ini, peran Tentara Nasional Indonesia (TNI) dinilai strategis dan krusial dalam konteks pertahanan negara. Namun demikian, pelibatan TNI dalam domain pertahanan siber masih menghadapi tantangan yuridis akibat belum adanya regulasi yang secara eksplisit dan komprehensif mengatur kewenangannya. Ketiadaan kerangka hukum yang memadai berpotensi menimbulkan tumpang tindih kewenangan antar instansi serta pelanggaran terhadap prinsip-prinsip hukum nasional dan internasional. Oleh karena itu, keterlibatan TNI dalam penanganan serangan siber harus dilandasi oleh aturan hukum yang jelas, terukur, dan sesuai dengan prinsip negara hukum serta supremasi sipil dalam tata kelola sektor pertahanan.

DAFTAR PUSTAKA

Peraturan Perundang-undangan

Undang-Undang Dasar Republik Indonesia 1945.
Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.

Jurnal

A. Suyanto, “Peran TNI dalam Penanggulangan Serangan Siber: Perspektif Hukum dan Keamanan Nasional”, *Jurnal Hukum & Keamanan, Vol. 15, No. 2*, (2020).
D. P. Fidler, “Cybersecurity and International Law: An Evolving Framework”, *Journal of International Affairs, Vol. 72, No.1* (2018) : 475-493

[17] https://www.jpnn.com/news/revisi-uu-tni-dinilai-hidupkan-dwifungsi-koalisi-masyarakat-sipil-desak-dpr-lakukan-ini, diakses tanggal 20 Juli 2025.

[18] Dr. Dave Akbarshah Fikarno Laksono, M.E., *Bahan Ajar pada saat Orasi Ilmiah pada Acara Pengukuhan Senat dan Alumni UNHAN RI*. PPT. Pengembangan Sistem Keamanan Siber untuk Pertahanan Negara: Tantangan dan Solusi.

Destya Fitri, dkk, "Peranan Manajemen Sekuriti Terhadap Keamanan Cyber Bersumber Nilai-Nilai Kebangsaan UUD 1945 Dalam Meningkatkan Efektivitas di Era Digitalisasi untuk Keamanan Nasional", *Menawan: Jurnal Riset dan Publikasi Ilmu Ekonomi, Vol. 3, No. 2,* (2024) : 273-283

I. Setiawan, "Doktrin Pertahanan Siber TNI dalam Menghadapi Ancaman Non-Konvensional", *Jurnal Pertahanan dan Keamanan, Vol. 24, No.3*, (2019).

M. Murphy, "Cyber Warfare and International Law: The Rules of Engagement". *International Law Review. Vol. 21, No. 4*, (2020).

Tamarell Vimy, dkk, Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal Kewarganegaraan, Vol. 6, No. 1*, (2022) : 2319-2327

Disertasi

Prabaswari, "Pengembangan Model Kapabilitas Tanggap Insiden Siber Sektor Pertahanan dalam Mengantisipasi Krisis Siber Nasional", *Disertasi, Program Studi Ilmu Pertahanan*, (Bogor : Unhan RI, 2025), dipublikasikan

Internet

https://nasional.kompas.com/read/2024/09/26/05150011/wacana-angkatan-siber-sejauh-mana-uu-pertahanan-dan-tni-direvisi-

https://news.republika.co.id/berita/qtre0w396/panglima-tni-berdayakan-semua-potensi-daya-siber-nasional

https://theconversation.com/pertahanan-siber-indonesia-jadi-tugas-penting-panglima-tni-yang-baru-171599

https://tniad.mil.id/dua-perwira-hukum-tni-ad-mengikuti-cyber-law-course-kerja-sama-ri-as/

https://www.antaranews.com/berita/2538541/profesionalisme-tni-pada-era-pertahanan-siber

https://www.jpnn.com/news/revisi-uu-tni-dinilai-hidupkan-dwifungsi-koalisi-masyarakat-sipil-desak-dpr-lakukan-ini

https://www.tni-au.mil.id/berita/detail/menjawab-tantangan-era-digital-tni-au-gelar-sosialisasi-aspek-hukum-penggunaan-siber-dalam-operasi-militer